Minimum disclosure proofs of knowledge

Journal of Computer and System Sciences

37, 156-189

DOI: 10.1016/0022-0000(88)90005-0

Citation Report

#	Article	IF	Citations
1	A probabilistic encryption using very high residuosity and its applications. , 0, , .		1
2	Limits on the provable consequences of one-way permutations. , 1989, , .		321
3	On hiding information from an oracle. Journal of Computer and System Sciences, 1989, 39, 21-50.	0.9	143
4	Efficient cryptographic schemes provably as secure as subset sum. , 1989, , .		33
5	Everything in NP can be argued in perfect zero-knowledge in a bounded number of rounds. Lecture Notes in Computer Science, 1989, , 123-136.	1.0	23
6	Secure circuit evaluation. Journal of Cryptology, 1990, 2, 1-12.	2.1	103
7	A discrete logarithm implementation of perfect zero-knowledge blobs. Journal of Cryptology, 1990, 2, 63-76.	2.1	57
8	Bit Commitment Using Pseudo-Randomness. , 1989, , 128-136.		95
9	Witness indistinguishable and witness hiding protocols. , 1990, , .		325
10	Lower bounds on random-self-reducibility. , 0, , .		16
11	Undeniable Signatures. Lecture Notes in Computer Science, 1990, , 212-216.	1.0	301
12	Subquadratic zero-knowledge. , 0, , .		3
13	Zero-Knowledge Undeniable Signatures (extended abstract). Lecture Notes in Computer Science, 1991, , 458-464.	1.0	162
14	Computationally convincing proofs of knowledge. , 1991, , 251-262.		7
15	Constant-round perfect zero-knowledge computationally convincing protocols. Theoretical Computer Science, 1991, 84, 23-52.	0.5	42
16	Elliptic curve implementation of zero-knowledge blobs. Journal of Cryptology, 1991, 4, 207-213.	2.1	26
17	Bit commitment using pseudorandomness. Journal of Cryptology, 1991, 4, 151-158.	2.1	513
18	Quantum Bit Commitment and Coin Tossing Protocols. , 1990, , 49-61.		45

#	Article	IF	Citations
19	Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. Journal of the ACM, 1991, 38, 690-728.	1.8	802
20	Superimposing encrypted data. Communications of the ACM, 1991, 34, 48-54.	3.3	14
21	Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing. , 1991, , 129-140.		1,177
22	Cryptographic Primitives And Quantum Theory. , 0, , .		1
24	Foundations of Secure Interactive Computing. , 1991, , 377-391.		133
25	A note on efficient zero-knowledge proofs and arguments (extended abstract). , 1992, , .		379
26	An almost-constant round interactive zero-knowledge proof. Information Processing Letters, 1992, 42, 81-87.	0.4	4
27	On the communication complexity of zero-knowledge proofs. Journal of Cryptology, 1993, 6, 65-85.	2.1	8
28	A perfect zero-knowledge proof system for a problem equivalent to the discrete logarithm. Journal of Cryptology, 1993, 6, 97-116.	2.1	26
29	A uniform-complexity treatment of encryption and zero-knowledge. Journal of Cryptology, 1993, 6, 21-53.	2.1	84
30	Random oracles are practical. , 1993, , .		2,900
31	A quantum bit commitment scheme provably unbreakable by both parties. , 0, , .		44
32	Two round ZKIP of knowledge for SAT and its applications. , 0, , .		0
33	Advances in Cryptology â€" EUROCRYPT â€™93. Lecture Notes in Computer Science, 1994, , .	1.0	20
34	Secure distributed computing: Theory and practice. Lecture Notes in Computer Science, 1994, , 53-73.	1.0	0
35	CS proofs. , 0, , .		117
36	The knowledge complexity of quadratic residuosity languages. Theoretical Computer Science, 1994, 132, 291-317.	0.5	27
37	Definitions and properties of zero-knowledge proof systems. Journal of Cryptology, 1994, 7, 1-32.	2.1	414

#	Article	IF	Citations
38	On the complexity of bounded-interaction and noninteractive zero-knowledge proofs. , 0, , .		10
39	Reducibility and completeness in multi-party private computations. , 0, , .		22
40	On monotone formula closure of SZK. , 0, , .		64
41	Distance-Bounding Protocols. , 1993, , 344-359.		408
42	Practical and provably secure release of a secret and exchange of signatures. Journal of Cryptology, 1995, 8, 201-222.	2.1	78
43	Group commitment protocol based on zero knowledge proofs. Computer Communications, 1995, 18, 654-656.	3.1	2
44	Subquadratic zero-knowledge. Journal of the ACM, 1995, 42, 1169-1193.	1.8	11
45	A secure and efficient conference key distribution system. Lecture Notes in Computer Science, 1995, , 275-286.	1.0	518
46	Receipt-Free Mix-Type Voting Scheme. Lecture Notes in Computer Science, 1995, , 393-403.	1.0	232
47	Designated confirmer signatures. Lecture Notes in Computer Science, 1995, , 86-91.	1.0	137
48	Efficient cryptographic schemes provably as secure as subset sum. Journal of Cryptology, 1996, 9, 199-216.	2.1	119
49	How to construct constant-round zero-knowledge proof systems for NP. Journal of Cryptology, 1996, 9, 167-189.	2.1	135
50	A low communication competitive interactive proof system for promised quadratic residuosity. Journal of Cryptology, 1996, 9, 101-109.	2.1	0
51	25 years of quantum cryptography. ACM SIGACT News, 1996, 27, 13-24.	0.1	48
52	On the Composition of Zero-Knowledge Proof Systems. SIAM Journal on Computing, 1996, 25, 169-192.	0.8	280
53	Designated Verifier Proofs and Their Applications. Lecture Notes in Computer Science, 1996, , 143-154.	1.0	480
54	Convertible group signatures. Lecture Notes in Computer Science, 1996, , 311-321.	1.0	28
56	On relationships between statistical zero-knowledge proofs. , 1996, , .		15

#	Article	IF	Citations
57	Adaptively secure multi-party computation. , 1996, , .		334
58	Adaptive zero knowledge and computational equivocation (extended abstract). , 1996, , .		22
59	Does parallel repetition lower the error in computationally sound protocols?. , 0, , .		41
60	Commodity-based cryptography (extended abstract). , 1997, , .		72
61	On the foundations of modern cryptography. Lecture Notes in Computer Science, 1997, , 46-74.	1.0	28
62	Quantum cryptanalysis of hash and claw-free functions. ACM SIGACT News, 1997, 28, 14-19.	0.1	69
63	New directions in cryptography: twenty some years later (or cryptograpy and complexity theory: a) Tj ETQq0 0 0 rgBT /Overlock 10 Tf 50		8
64	Multi party computations. , 1997, , .		151
65	Linear zero-knowledge---a note on efficient zero-knowledge proofs and arguments. , 1997, , .		35
66	Statistical zero knowledge protocols to prove modular polynomial relations. Lecture Notes in Computer Science, 1997, , 16-30.	1.0	308
67	Efficient group signature schemes for large groups. Lecture Notes in Computer Science, 1997, , 410-424.	1.0	645
68	Probabilistic proof systems â€" A survey. Lecture Notes in Computer Science, 1997, , 595-611.	1.0	2
69	A General Zero-Knowledge Scheme. Designs, Codes, and Cryptography, 1997, 12, 13-37.	1.0	1
70	A language-dependent cryptographic primitive. Journal of Cryptology, 1997, 10, 37-49.	2.1	32
71	On the existence of statistically hiding bit commitment schemes and fail-stop signatures. Journal of Cryptology, 1997, 10, 163-194.	2.1	47
72	Practical proofs of knowledge without relying on theoretical proofs of membership on languages. Theoretical Computer Science, 1997, 181, 317-335.	0.5	0
73	On the complexity of interactive proofs with bounded communication. Information Processing Letters, 1998, 67, 205-214.	0.4	57
74	Perfect Zero-Knowledge Arguments for NP Using Any One-Way Permutation. Journal of Cryptology, 1998, 11, 87-108.	2.1	113

#	Article	IF	Citations
75	â€œParamita wisdomâ€•password authentication scheme without verification tables. Journal of Systems and Software, 1998, 42, 45-57.	3.3	46
76	A new public key cryptosystem based on higher residues. , 1998, , .		219
77	On the existence of 3-round zero-knowledge protocols. Lecture Notes in Computer Science, 1998, , 408-423.	1.0	101
78	Server-assisted cryptography. , 1998, , .		14
79	Advances in Cryptology â€” ASIACRYPTâ€™98. Lecture Notes in Computer Science, 1998, , .	1.0	12
80	Identity escrow. Lecture Notes in Computer Science, 1998, , 169-185.	1.0	121
82	Sequential iteration of interactive arguments and an efficient zero-knowledge argument for NP. Lecture Notes in Computer Science, 1998, , 772-783.	1.0	8
83	A compact and fast hybrid signature scheme for multicast packet authentication. , 1999, , .		115
84	Using smartcards to secure a personalized gambling device. , 1999, , .		2
85	On the Concurrent Composition of Zero-Knowledge Proofs. Lecture Notes in Computer Science, 1999, , 415-431.	1.0	94
86	Batching proofs of knowledge and its applications. , 1999, , .		3
88	Divertible and Subliminal-Free Zero-Knowledge Proofs for Languages. Journal of Cryptology, 1999, 12, 197-223.	2.1	10
89	Efficient Commitment Schemes with Bounded Sender and Unbounded Receiver. Journal of Cryptology, 1999, 12, 77-89.	2.1	11
90	Modern Cryptography, Probabilistic Proofs and Pseudorandomness. Algorithms and Combinatorics, 1999, , .	0.6	130
91	Knowledge-proof based versatile smart card verification protocol. Computer Communication Review, 2000, 30, 39-44.	1.5	16
92	On Relationships between Statistical Zero-Knowledge Proofs. Journal of Computer and System Sciences, 2000, 60, 47-108.	0.9	44
93	RSA-Based Undeniable Signatures. Journal of Cryptology, 2000, 13, 397-416.	2.1	67
94	Short Non-Interactive Cryptographic Proofs. Journal of Cryptology, 2000, 13, 449-472.	2.1	30

#	Article	IF	Citations
95	Advances in Cryptology â€" EUROCRYPT 2000. Lecture Notes in Computer Science, 2000, , .	1.0	8
96	Resettable zero-knowledge (extended abstract). , 2000, , .		109
97	A Group Signature Scheme with Improved Efficiency (Extended Abstract). Lecture Notes in Computer Science, 2000, , 160-174.	1.0	84
98	Reducibility and Completeness in Private Computations. SIAM Journal on Computing, 2000, 29, 1189-1208.	0.8	41
99	Computationally Sound Proofs. SIAM Journal on Computing, 2000, 30, 1253-1298.	0.8	260
101	Optimistic fair exchange of digital signatures. IEEE Journal on Selected Areas in Communications, 2000, 18, 593-610.	9.7	333
102	Robust Non-interactive Zero Knowledge. Lecture Notes in Computer Science, 2001, , 566-598.	1.0	156
103	Universally composable security: a new paradigm for cryptographic protocols. , 2001, , .		1,616
104	Concurrent and resettable zero-knowledge in poly-loalgorithm rounds. , 2001, , .		79
106	Paillier's cryptosystem revisited. , 2001, , .		58
107	Advances in Cryptology â€" EUROCRYPT 2001. Lecture Notes in Computer Science, 2001, , .	1.0	17
109	Black-box concurrent zero-knowledge requires ilde {Î©} (logn) rounds. , 2001, , .		70
110	Universal arguments and their applications. , 0, , .		44
111	Information Security. Lecture Notes in Computer Science, 2002, , .	1.0	1
112	Strict polynomial-time in simulation and extraction. , 2002, , .		41
113	Universally composable two-party and multi-party secure computation. , 2002, , .		334
114	Concurrent zero-knowledge with timing, revisited. , 2002, , .		29
115	Concurrent zero knowledge with logarithmic round-complexity. , 0, , .		59

#	Article	IF	Citations
116	Black-Box Concurrent Zero-Knowledge Requires (Almost) Logarithmically Many Rounds. SIAM Journal on Computing, 2002, 32, 1-47.	0.8	41
117	On interactive proofs with a laconic prover. Computational Complexity, 2002, 11, 1-53.	0.2	63
118	A Note on Negligible Functions. Journal of Cryptology, 2002, 15, 271-284.	2.1	43
119	Constructions and Bounds for Unconditionally Secure Non-Interactive Commitment Schemes. Designs, Codes, and Cryptography, 2002, 26, 97-110.	1.0	23
120	Watermark detection with zero-knowledge disclosure. Multimedia Systems, 2003, 9, 266-278.	3.0	33
121	Lower bounds for non-black-box zero knowledge. , 0, , .		22
123	Universal Designated-Verifier Signatures. Lecture Notes in Computer Science, 2003, , 523-542.	1.0	138
124	A Simple Public-Key Cryptosystem with a Double Trapdoor Decryption Mechanism and Its Applications. Lecture Notes in Computer Science, 2003, , 37-54.	1.0	191
125	The Knowledge-of-Exponent Assumptions and 3-Round Zero-Knowledge Protocols. Lecture Notes in Computer Science, 2004, , 273-289.	1.0	151
126	Concurrent zero-knowledge. Journal of the ACM, 2004, 51, 851-898.	1.8	108
127	An Unconditional Study of Computational Zero Knowledge. , 0, , .		16
128	Overcoming the obstacles of zero-knowledge watermark detection. , 2004, , .		15
129	Strict Polynomial-Time in Simulation and Extraction. SIAM Journal on Computing, 2004, 33, 783-818.	0.8	28
130	Oblivious polynomial evaluation and oblivious neural learning. Theoretical Computer Science, 2005, 341, 39-54.	0.5	19
131	Interactive and Probabilistic Proof of Mobile Code Safety. Automated Software Engineering, 2005, 12, 237-257.	2.2	3
132	Lower Bounds For Concurrent Zero Knowledge*. Combinatorica, 2005, 25, 217-249.	0.6	3
133	Complementing zero-knowledge watermark detection: Proving properties of embedded information without revealing it. Multimedia Systems, 2005, 11, 143-158.	3.0	8
134	Signcryption with Non-interactive Non-repudiation. Designs, Codes, and Cryptography, 2005, 37, 81-109.	1.0	19

#	Article	IF	Citations
135	On the Key Exposure Problem in Chameleon Hashes. Lecture Notes in Computer Science, 2005, , 165-179.	1.0	109
136	A Privacy-Protecting Coupon System. Lecture Notes in Computer Science, 2005, , 93-108.	1.0	19
137	Mercurial Commitments with Applications to Zero-Knowledge Sets. Lecture Notes in Computer Science, 2005, , 422-439.	1.0	39
138	New and improved constructions of non-malleable cryptographic protocols. , 2005, , .		82
139	An abuse-free fair contract signing protocol based on the RSA signature. , 2005, , .		15
143	Fingerprinting protocol for images based on additive homomorphic property. IEEE Transactions on Image Processing, 2005, 14, 2129-2139.	6.0	106
144	Hybrid Trapdoor Commitments and Their Applications. Lecture Notes in Computer Science, 2005, , 298-310.	1.0	13
145	Impossible Differential Attack. , 2005, , 286-287.		0
147	Statistical Zero-Knowledge Arguments for NP from Any One-Way Function. , 2006, , .		27
148	An Unconditional Study of Computational Zero Knowledge. SIAM Journal on Computing, 2006, 36, 1160-1214.	0.8	21
149	Watermarking Security: A Survey. Lecture Notes in Computer Science, 2006, , 41-72.	1.0	49
150	Security and composition of cryptographic protocols. ACM SIGACT News, 2006, 37, 67-92.	0.1	39
151	Zero-knowledge against quantum attacks. , 2006, , .		37
152	Addressing the shortcomings of one-way chains. , 2006, , .		9
153	Practical secrecy-preserving, verifiably correct and trustworthy auctions. , 2006, , .		25
155	Efficient Protocols Achieving the Commitment Capacity of Noisy Correlations. , 2006, , .		20
158	A New Interactive Hashing Theorem. Computational Complexity, IEEE Annual Conference on, 2007, , .	0.0	15
159	Statistically-hiding commitment from any one-way function. , 2007, , .		37

#	Article	IF	Citations
160	An efficient parallel repetition theorem for Arthur-Merlin games. , 2007, , .		22
161	Reexamination of quantum bit commitment: The possible and the impossible. Physical Review A, 2007, 76, .	1.0	73
163	Efficient Arguments without Short PCPs. Computational Complexity, IEEE Annual Conference on, 2007, , .	0.0	79
164	Highly Efficient Secrecy-Preserving Proofs of Correctness of Computations and Applications. , 2007, , .		14
165	Constant-Round Restricted-Verifier Zero-Knowledge with Polynomial Precision. , 2007, , .		2
166	Finding Collisions in Interactive Protocols - A Tight Lower Bound on the Round Complexity of Statistically-Hiding Commitments. , 2007, , .		44
167	An Improved Method of Differential Fault Analysis on the SMS4 Cryptosystem. , 2007, , .		10
168	Hybrid commitments and their applications to zero-knowledge proof systems. Theoretical Computer Science, 2007, 374, 229-260.	0.5	19
171	Tight bounds for the multiplicative complexity of symmetric functions. Theoretical Computer Science, 2008, 396, 223-246.	0.5	19
172	Concurrent Nonmalleable Commitments. SIAM Journal on Computing, 2008, 37, 1891-1925.	0.8	26
173	On Monotone Formula Composition of Perfect Zero-Knowledge Languages. SIAM Journal on Computing, 2008, 38, 1300-1329.	0.8	2
174	New and Improved Constructions of Nonmalleable Cryptographic Protocols. SIAM Journal on Computing, 2008, 38, 702-752.	0.8	35
175	5-Round Computational Zero-Knowledge Proof with Negligible Error Probability for Any NP from Any One-Way Permutation. , 2008, , .		0
176	The Marriage of Cryptography and Watermarking â€" Beneficial and Challenging for Secure Watermarking and Detection. Lecture Notes in Computer Science, 2008, , 2-18.	1.0	12
177	Digital Watermarking. Lecture Notes in Computer Science, 2008, , .	1.0	18
179	Polylogarithmic two-round argument systems. Journal of Mathematical Cryptology, 2008, 2, .	0.4	20
180	Secure Relativistic Bit Commitment with Fixed Channel Capacity. , 2008, , .		0
181	A practical scheme for quantum oblivious transfer and private database sampling. Proceedings of SPIE, 2008, , .	0.8	0

#	Article	IF	Citations
183	Are PCPs Inherent in Efficient Arguments?. , 2009, , .		6
184	Non-malleability amplification. , 2009, , .		47
185	A Further Improved Online/Offline Signature Scheme. Fundamenta Informaticae, 2009, 91, 523-532.	0.3	2
186	Precise zero-knowledge arguments with poly-logarithmic efficiency. Journal of Shanghai Jiaotong University (Science), 2009, 14, 584-589.	0.5	0
187	Reducing Complexity Assumptions forÂStatistically-Hiding Commitment. Journal of Cryptology, 2009, 22, 283-310.	2.1	4
188	New Approaches for Deniable Authentication. Journal of Cryptology, 2009, 22, 572-615.	2.1	35
189	Efficient Non-malleable Commitment Schemes. Journal of Cryptology, 2009, 22, 530.	2.1	14
190	Simplified design for concurrent statistical zero-knowledge arguments. Tsinghua Science and Technology, 2009, 14, 255-263.	4.1	0
191	Zero-Knowledge against Quantum Attacks. SIAM Journal on Computing, 2009, 39, 25-58.	0.8	103
192	Digital Watermarking. Lecture Notes in Computer Science, 2009, , .	1.0	3
193	Universal Arguments and their Applications. SIAM Journal on Computing, 2009, 38, 1661-1694.	0.8	64
194	Statistically Hiding Commitments and Statistical Zero-Knowledge Arguments from Any One-Way Function. SIAM Journal on Computing, 2009, 39, 1153-1218.	0.8	61
195	Quantum private data sampling. Proceedings of SPIE, 2009, , .	0.8	0
196	On the Implementation of Spread Spectrum Fingerprinting in Asymmetric Cryptographic Protocol. Eurasip Journal on Information Security, 2010, 2010, 1-11.	2.2	13
197	Threshold cryptography. European Transactions on Telecommunications, 1994, 5, 449-458.	1.2	223
198	Are PCPs Inherent in Efficient Arguments?. Computational Complexity, 2010, 19, 265-304.	0.2	11
199	Long-Term Security and Universal Composability. Journal of Cryptology, 2010, 23, 594-671.	2.1	16
200	Survey on anonymous communications in computer networks. Computer Communications, 2010, 33, 420-431.	3.1	84

#	Article	IF	Citations
201	Precise bounded-concurrent zero-knowledge proofs for NP. Science China Information Sciences, 2010, 53, 1738-1752.	2.7	0
202	On sequential composition of precise zero-knowledge. Journal of Shanghai Jiaotong University (Science), 2010, 15, 43-48.	0.5	0
203	Efficient proxy signatures based on trapdoor hash functions. IET Information Security, 2010, 4, 322.	1.1	12
204	An Abuse-Free Fair Contract-Signing Protocol Based on the RSA Signature. IEEE Transactions on Information Forensics and Security, 2010, 5, 158-168.	4.5	38
205	Recent Fingerprinting Techniques with Cryptographic Protocol. , 2010, , .		1
206	Network Security. , 2010, , .		7
207	A pull model IPv6 Duplicate Address Detection. , 2010, , .		12
208	A New Sampling Protocol and Applications to Basing Cryptographic Primitives on the Hardness of NP. , 2010, , .		11
209	Selected Areas in Cryptography. Lecture Notes in Computer Science, 2011, , .	1.0	7
210	Identity-based trapdoor mercurial commitments and applications. Theoretical Computer Science, 2011, 412, 5498-5512.	0.5	5
211	Memory Delegation. Lecture Notes in Computer Science, 2011, , 151-168.	1.0	68
212	Efficient Non-Malleable Commitment Schemes. Journal of Cryptology, 2011, 24, 203-244.	2.1	5
213	Short Undeniable Signatures Based onÂGroupÂHomomorphisms. Journal of Cryptology, 2011, 24, 545-587.	2.1	6
214	New receipt-free voting scheme using double-trapdoor commitmentâ˜†. Information Sciences, 2011, 181, 1493-1502.	4.0	24
215	Achieving nonâ€transferability in credential systems using hidden biometrics. Security and Communication Networks, 2011, 4, 195-206.	1.0	10
216	Constant-round non-malleable commitments from any one-way function. , 2011, , .		52
217	Provable Security. Lecture Notes in Computer Science, 2011, , .	1.0	0
218	A Parallel Repetition Theorem for Constant-Round Arthur-Merlin Proofs. ACM Transactions on Computation Theory, 2012, 4, 1-22.	0.4	4

#	Article	IF	Citations
219	From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again. , 2012, , .		255
220	Meta-envy-free Cake-cutting and Pie-cutting Protocols. Journal of Information Processing, 2012, 20, 686-693.	0.3	2
221	A Trapdoor Hash Based Mechanism for Stream Authentication. IEEE Transactions on Dependable and Secure Computing, 2012, , 1-1.	3.7	5
222	A dynamic fuzzy commitment scheme using multiple commitments. , 2012, , .		1
223	New Techniques for Noninteractive Zero-Knowledge. Journal of the ACM, 2012, 59, 1-35.	1.8	125
224	Succinct Arguments from Multi-prover Interactive Proofs and Their Efficiency Benefits. Lecture Notes in Computer Science, 2012, , 255-272.	1.0	36
225	The Curious Case of Non-Interactive Commitments â€" On the Power of Black-Box vs. Non-Black-Box Use of Primitives. Lecture Notes in Computer Science, 2012, , 701-718.	1.0	20
226	Efficient ID-based non-malleable trapdoor commitment. Computers and Electrical Engineering, 2012, 38, 1647-1657.	3.0	2
227	Study on poll-site voting and verification systems. Computers and Security, 2012, 31, 989-1010.	4.0	6
228	On the impossibility of non-static quantum bit commitment between two parties. Quantum Information Processing, 2012, 11, 519-527.	1.0	9
229	Leakproof secret sharing protocols with applications to group identification scheme. Science China Information Sciences, 2012, 55, 1172-1185.	2.7	4
230	Which Languages Have 4-Round Zero-Knowledge Proofs?. Journal of Cryptology, 2012, 25, 41-56.	2.1	8
231	Parallel Repetition of Computationally Sound Protocols Revisited. Journal of Cryptology, 2012, 25, 116-135.	2.1	4
232	Mercurial Commitments with Applications to Zero-Knowledge Sets. Journal of Cryptology, 2013, 26, 251-279.	2.1	13
234	Succinct Non-interactive Arguments via Linear Interactive Proofs. Lecture Notes in Computer Science, 2013, , 315-333.	1.0	161
235	Quadratic Span Programs and Succinct NIZKs without PCPs. Lecture Notes in Computer Science, 2013, , 626-645.	1.0	420
236	SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge. Lecture Notes in Computer Science, 2013, , 90-108.	1.0	304
237	Fast reductions from RAMs to delegatable succinct constraint satisfaction problems. , 2013, , .		53

#	Article	IF	Citations
238	Off-line/on-line signatures revisited: a general unifying paradigm, efficient threshold variants and experimental results. International Journal of Information Security, 2013, 12, 439-465.	2.3	1
239	A lightweight argument system with efficient verifier. , 2013, , .		0
240	A multiple fuzzy commitment scheme. , 2013, , .		0
241	Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation. IEEE Signal Processing Magazine, 2013, 30, 82-105.	4.6	255
242	Building a privacy-preserving semantic overlay for Peer-to-Peer networks. , 2013, , .		7
243	Delegation of computation with verification outsourcing. , 2013, , .		6
244	Simultaneous Resettability from One-Way Functions. , 2013, , .		14
245	Verifying the correctness of remote executions. , 2013, , .		2
246	Guest column. ACM SIGACT News, 2013, 44, 50-69.	0.1	1
247	Recursive composition and bootstrapping for SNARKS and proof-carrying data. , 2013, , .		164
248	Verifying computations with state. , 2013, , .		97
249	A Hybrid Architecture for Interactive Verifiable Computation. , 2013, , .		85
250	A Survey of Noninteractive Zero Knowledge Proof System and Its Applications. Scientific World Journal, The, 2014, 2014, 1-7.	0.8	12
251	Secure Multiparty Computations on Bitcoin. , 2014, , .		235
252	Belief manipulation and message meaning for protocol analysis. Security Informatics, 2014, 3, .	2.5	0
253	A brief review on quantum bit commitment. Proceedings of SPIE, 2014, , .	0.8	3
255	Towards secure end-to-end data aggregation in AMI through delayed-integrity-verification. , 2014, , .		1
256	A Survey on Zero-Knowledge Proofs. Advances in Computers, 2014, , 25-69.	1.2	7

#	Article	IF	Citations
257	A New Interactive Hashing Theorem. Journal of Cryptology, 2014, 27, 109-138.	2.1	1
258	Cheat sensitive quantum bit commitment via pre- and post-selected quantum states. Quantum Information Processing, 2014, 13, 141-149.	1.0	23
259	A mobile biometric-based e-voting scheme. , 2014, , .		1
260	Delegation of Computation with Verification Outsourcing Using GENI Infrastructure. , 2014, , .		0
261	New Algorithms for Secure Outsourcing of Modular Exponentiations. IEEE Transactions on Parallel and Distributed Systems, 2014, 25, 2386-2396.	4.0	241
262	Privacy-Aware Smart Metering: A Survey. IEEE Communications Surveys and Tutorials, 2014, 16, 1732-1745.	24.8	68
263	CooPeD: Co-owned Personal Data management. Computers and Security, 2014, 47, 41-65.	4.0	12
264	A lightweight possession proof scheme for outsourced files in mobile cloud computing based on chameleon hash function. International Journal of Computational Science and Engineering, 2014, 9, 339.	0.4	12
265	Arbitrarily Long Relativistic Bit Commitment. Physical Review Letters, 2015, 115, 250501.	2.9	19
266	A privacy-preserving e-participation framework allowing citizen opinion analysis. Electronic Government, 2015, 11, 185.	0.1	7
267	Finding Collisions in Interactive Protocols---Tight Lower Bounds on the Round and Communication Complexities of Statistically Hiding Commitments. SIAM Journal on Computing, 2015, 44, 193-242.	0.8	26
268	A Cryptographic Moving-Knife Cake-Cutting Protocol with High Social Surplus. Journal of Information Processing, 2015, 23, 299-304.	0.3	1
270	Privacy-Aware Smart Metering: A Survey. IEEE Communications Surveys and Tutorials, 2015, 17, 1088-1101.	24.8	80
271	Efficient RAM and Control Flow in Verifiable Outsourced Computation. , 2015, , .		81
272	Quantum bit commitment with cheat sensitive binding and approximate sealing. Journal of Physics A: Mathematical and Theoretical, 2015, 48, 135302.	0.7	4
273	Spreading Alerts Quietly and the Subgroup Escape Problem. Journal of Cryptology, 2015, 28, 796-819.	2.1	2
275	Verifying computations without reexecuting them. Communications of the ACM, 2015, 58, 74-84.	3.3	93
276	Constant-Round Nonmalleable Commitments from Any One-Way Function. Journal of the ACM, 2015, 62, 1-30.	1.8	10

#	Article	IF	Citations
277	Block Programs. , 2015, , .		1
278	UWB rapid-bit-exchange system for distance bounding. , 2015, , .		17
279	Computationally-Sound Proofs. , 0, , 214-268.		0
280	On the Existence of Extractable One-Way Functions. SIAM Journal on Computing, 2016, 45, 1910-1952.	0.8	13
281	SAriadne: A secure source routing protocol to prevent hidden-channel attacks. , 2016, , .		2
282	Hash First, Argue Later. , 2016, , .		42
283	Privacy-preserving distributed location proof generating system. China Communications, 2016, 13, 203-218.	2.0	4
284	Verifiable ASICs. , 2016, , .		45
285	Adaptive Hardness and Composable Security in the Plain Model from Standard Assumptions. SIAM Journal on Computing, 2016, 45, 1793-1834.	0.8	6
286	Information Theoretic Security. Lecture Notes in Computer Science, 2016, , .	1.0	1
287	Information Security Practice and Experience. Lecture Notes in Computer Science, 2016, , .	1.0	1
288	Concurrent Knowledge Extraction in Public-Key Models. Journal of Cryptology, 2016, 29, 156-219.	2.1	1
289	Introduction to Secure Outsourcing Computation. Synthesis Lectures on Information Security Privacy and Trust, 2016, 8, 1-93.	0.3	8
290	Privacy Preserving Spam Email Filtering Based on Somewhat Homomorphic Using Functional Encryption. Advances in Intelligent Systems and Computing, 2016, , 579-585.	0.5	2
291	Enabling the Sharing Economy. , 2017, , .		60
292	Hashing Garbled Circuits for Free. Lecture Notes in Computer Science, 2017, , 456-485.	1.0	4
293	Oblivious transfer based on single-qubit rotations. Journal of Physics A: Mathematical and Theoretical, 2017, 50, 205301.	0.7	6
294	The Need for Audit-Capable E-Voting Systems. , 2017, , .		4

#	Article	IF	Citations
296	Identity-Based Encryption from the Diffie-Hellman Assumption. Lecture Notes in Computer Science, 2017, , 537-569.	1.0	105
297	Resettably-Sound Resettable Zero Knowledge in Constant Rounds. Lecture Notes in Computer Science, 2017, , 111-138.	1.0	3
298	Redactable Blockchain â€" or â€" Rewriting History in Bitcoin and Friends. , 2017, , .		214
299	Quantum Communication and Cryptography. Quantum Science and Technology, 2017, , 201-220.	1.5	1
300	Delegation of Computation with Verification Outsourcing: Curious Verifiers. IEEE Transactions on Parallel and Distributed Systems, 2017, 28, 717-730.	4.0	6
301	Efficiency lower bounds for commit-and-prove constructions. , 2017, , .		0
302	Full Accounting for Verifiable Outsourcing. , 2017, , .		38
303	Quasi-Optimal SNARGs via Linear Multi-Prover Interactive Proofs. Lecture Notes in Computer Science, 2018, , 222-255.	1.0	25
304	SnÃ¥rkl: Somewhat Practical, Pretty Much Declarative Verifiable Computing in Haskell. Lecture Notes in Computer Science, 2018, , 36-52.	1.0	1
305	Practical Aspects of Declarative Languages. Lecture Notes in Computer Science, 2018, , .	1.0	1
306	Using Malleable Signatures to Allow Multi-Show Capability in Digital Credentials. Internatinoal Journal of Sensor Networks and Data Communications, 2018, 07, .	0.1	1
307	Lattice-Based zk-SNARKs from Square Span Programs. , 2018, , .		27
308	Linkable Group Signature for Auditing Anonymous Communication. Lecture Notes in Computer Science, 2018, , 304-321.	1.0	17
309	Statistical Witness Indistinguishability (and more) in Two Messages. Lecture Notes in Computer Science, 2018, , 34-65.	1.0	25
310	Chameleon-Hashes with Dual Long-Term Trapdoors and Their Applications. Lecture Notes in Computer Science, 2018, , 11-32.	1.0	11
312	Privacy in e-Shopping Transactions: Exploring and Addressing the Trade-Offs. Lecture Notes in Computer Science, 2018, , 206-226.	1.0	0
313	Subvector Commitments with Application to Succinct Arguments. Lecture Notes in Computer Science, 2019, , 530-560.	1.0	53
314	Probabilistic Smart Contracts: Secure Randomness on the Blockchain. , 2019, , .		45

#	Article	IF	Citations
315	Privacy-Preserving Solutions for Blockchain: Review and Challenges. IEEE Access, 2019, 7, 164908-164940.	2.6	211
316	A tutorial on concurrent zero-knowledge. , 2019, , .		0
317	ILC: a calculus for composable, computational cryptography. , 2019, , .		9
318	Algorithmic Game Theory. Lecture Notes in Computer Science, 2019, , .	1.0	0
319	Aurora: Transparent Succinct Arguments for R1CS. Lecture Notes in Computer Science, 2019, , 103-128.	1.0	139
320	Achieving liability in anonymous communication: Auditing and tracing. Computer Communications, 2019, 145, 1-13.	3.1	6
321	S-money: virtual tokens for a relativistic economy. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, 2019, 475, 20190170.	1.0	9
322	Privacy-preserving metering in smart grid for billing, operational metering, and incentive-based schemes: A survey. Computers and Security, 2019, 84, 148-165.	4.0	29
323	Non-black-box Simulation in the Fully Concurrent Setting, Revisited. Journal of Cryptology, 2019, 32, 393-434.	2.1	1
324	Improved generic construction of chameleon hash to group elements. Journal of the Chinese Institute of Engineers, Transactions of the Chinese Institute of Engineers,Series A/Chung-kuo Kung Ch'eng Hsuch K'an, 2019, 42, 29-38.	0.6	1
325	Verifying quantum computations at scale: A cryptographic leash on quantum devices. Bulletin of the American Mathematical Society, 2019, 57, 39-76.	0.8	2
326	Ã†GIS. , 2019, , .		8
327	Cryptographic primitives in blockchains. Journal of Network and Computer Applications, 2019, 127, 43-58.	5.8	134
328	A Methodology for Retrofitting Privacy and Its Application to e-Shopping Transactions. , 2019, , 143-183.		1
330	On the Power of Secure Two-Party Computation. Journal of Cryptology, 2020, 33, 271-318.	2.1	1
331	Concise ID-based mercurial functional commitments and applications to zero-knowledge sets. International Journal of Information Security, 2020, 19, 453-464.	2.3	0
332	Efficient chameleon hash functions in the enhanced collision resistant model. Information Sciences, 2020, 510, 155-164.	4.0	30
333	A (Zero-Knowledge) Vector Commitment with Sum Binding and its Applications. Computer Journal, 2020, 63, 633-647.	1.5	4

#	Article	IF	Citations
334	Fair payments for verifiable cloud services using smart contracts. Computers and Security, 2020, 90, 101712.	4.0	19
335	Sharing Economy: Implementing Decentralized Privacy-Preserving Parking System. , 2020, , .		1
336	Blockchain-Enabled Federated Learning With Mechanism Design. IEEE Access, 2020, 8, 219744-219756.	2.6	36
337	A Framework for Decentralized Private Random State Generation and Maintenance for Multiplayer Gaming Over Blockchain. , 2020, , .		0
338	An Adaptive Authenticated Data Structure With Privacy-Preserving for Big Data Stream in Cloud. IEEE Transactions on Information Forensics and Security, 2020, 15, 3295-3310.	4.5	36
339	A review on smart metering infrastructure. International Journal of Energy Technology and Policy, 2020, 16, 277.	0.1	3
341	On the Commitment Capacity of Unfair Noisy Channels. IEEE Transactions on Information Theory, 2020, 66, 3745-3752.	1.5	11
342	A Private Quantum Bit String Commitment. Entropy, 2020, 22, 272.	1.1	2
343	Statistical Concurrent Non-Malleable Zero-Knowledge from One-Way Functions. Journal of Cryptology, 2020, 33, 1318-1361.	2.1	1
344	Cryptographic Framework for Role Control Remedy: A Secure Role Engineering mechanism for Single Authority Organizations. Future Generation Computer Systems, 2021, 117, 245-258.	4.9	2
345	Zilch: A Framework for Deploying Transparent Zero-Knowledge Proofs. IEEE Transactions on Information Forensics and Security, 2021, 16, 3269-3284.	4.5	11
346	On Using zk-SNARKs and zk-STARKs in Blockchain-Based Identity Management. Lecture Notes in Computer Science, 2021, , 130-145.	1.0	6
347	A coercion-resistant blockchain-based E-voting protocol with receipts. Advances in Mathematics of Communications, 2023, 17, 500-521.	0.4	1
348	Group Encryption: Full Dynamicity, Message Filtering and Code-Based Instantiation. Lecture Notes in Computer Science, 2021, , 678-708.	1.0	3
349	A Security Analysis of Blockchain-Based Did Services. IEEE Access, 2021, 9, 22894-22913.	2.6	15
350	Single-to-Multi-theorem Transformations for Non-interactive Statistical Zero-Knowledge. Lecture Notes in Computer Science, 2021, , 205-234.	1.0	3
351	Zero-Knowledge Proofs for Committed Symmetric Boolean Functions. Lecture Notes in Computer Science, 2021, , 339-359.	1.0	1
353	Private and Trustworthy Distributed Lending Model Using Hyperledger Besu. SN Computer Science, 2021, 2, 1.	2.3	6

#	Article	IF	Citations
354	Identity-based Encryption from the Diffie-Hellman Assumption. Journal of the ACM, 2021, 68, 1-46.	1.8	2
355	Redactable Blockchain Supporting Supervision and Self-Management. , 2021, , .		25
356	Secure Chaff-less Fuzzy Vault for Face Identification Systems. ACM Transactions on Multimedia Computing, Communications and Applications, 2021, 17, 1-22.	3.0	10
357	Commitment Capacity under Cost Constraints. , 2021, , .		4
358	A Survey of Self-Sovereign Identity Ecosystem. Security and Communication Networks, 2021, 2021, 1-26.	1.0	40
359	Commitment over Compound Binary Symmetric Channels. , 2021, , .		7
361	A â€œParadoxicalâ€•Indentity-Based Signature Scheme Resulting from Zero-Knowledge. Lecture Notes in Computer Science, 1990, , 216-231.	1.0	254
362	Disposable Zero-Knowledge Authentications and Their Applications to Untraceable Electronic Cash. , 1989, , 481-496.		65
363	Efficient Identification Schemes Using Two Prover Interactive Proofs. , 1989, , 498-506.		8
364	On the concrete complexity of zero-knowledge proofs. , 1989, , 507-525.		5
365	The Spymasters Double-Agent Problem. , 1989, , 591-602.		19
366	Proving Ownership of Digital Content. Lecture Notes in Computer Science, 2000, , 117-133.	1.0	18
367	Reducing Complexity Assumptions for Statistically-Hiding Commitment. Lecture Notes in Computer Science, 2005, , 58-77.	1.0	23
368	Concurrent Zero Knowledge in the Public-Key Model. Lecture Notes in Computer Science, 2005, , 816-827.	1.0	15
370	Spreading Alerts Quietly and the Subgroup Escape Problem. Lecture Notes in Computer Science, 2005, , 253-272.	1.0	4
371	Universal Designated Verifier Signature Proof (or How to Efficiently Prove Knowledge of a) Tj ETQq1 1 0.784314 rgBT /Overlock 10 Tf 50	1.0	26
372	Short Undeniable Signatures Without Random Oracles: The Missing Link. Lecture Notes in Computer Science, 2005, , 283-296.	1.0	25
373	Ring-Based Anonymous Fingerprinting Scheme. Lecture Notes in Computer Science, 2005, , 1080-1085.	1.0	5

#	Article	IF	Citations
374	Practical Zero-Knowledge Arguments from Î£-Protocols. Lecture Notes in Computer Science, 2005, , 288-298.	1.0	1
376	Concurrent Zero Knowledge Without Complexity Assumptions. Lecture Notes in Computer Science, 2006, , 1-20.	1.0	20
377	Mercurial Commitments: Minimal Assumptions and Efficient Constructions. Lecture Notes in Computer Science, 2006, , 120-144.	1.0	29
378	Efficient Zero Knowledge on the Internet. Lecture Notes in Computer Science, 2006, , 22-33.	1.0	13
379	A Cryptographic Framework for the Controlled Release of Certified Data. Lecture Notes in Computer Science, 2006, , 20-42.	1.0	38
380	Non-interactive Distributed-Verifier Proofs and Proving Relations among Commitments. Lecture Notes in Computer Science, 2002, , 206-224.	1.0	13
381	A Signature Scheme with Efficient Protocols. Lecture Notes in Computer Science, 2003, , 268-289.	1.0	358
382	Equivocable and Extractable Commitment Schemes. Lecture Notes in Computer Science, 2003, , 74-87.	1.0	7
383	Convertible Undeniable Signatures. , 1990, , 189-205.		110
384	Multi-Language Zero Knowledge Interactive Proof Systems. , 1990, , 339-352.		1
385	How to Utilize the Randomness of Zero-Knowledge Proofs. , 1990, , 456-475.		19
386	One-Way Group Actions. , 1990, , 94-107.		21
387	Simulatable Commitments and Efficient Concurrent Zero-Knowledge. Lecture Notes in Computer Science, 2003, , 140-159.	1.0	17
388	Cryptography 2000Â±10. Lecture Notes in Computer Science, 2001, , 63-85.	1.0	5
389	Efficient Non-malleable Commitment Schemes. Lecture Notes in Computer Science, 2000, , 413-431.	1.0	58
390	Soundness in the Public-Key Model. Lecture Notes in Computer Science, 2001, , 542-565.	1.0	62
391	A Simple Method for Generating and Sharing Pseudo-Random Functions, with Applications to Clipper-like Key Escrow Systems. Lecture Notes in Computer Science, 1995, , 185-196.	1.0	34
392	Fair Cryptosystems, Revisited. Lecture Notes in Computer Science, 1995, , 208-221.	1.0	40

#	Article	IF	Citations
393	Improved Efficient Arguments. Lecture Notes in Computer Science, 1995, , 311-324.	1.0	30
394	Identification Protocols Secure against Reset Attacks. Lecture Notes in Computer Science, 2001, , 495-511.	1.0	56
395	How to Convert the Flavor of a Quantum Bit Commitment. Lecture Notes in Computer Science, 2001, , 60-77.	1.0	20
396	Necessary and Sufficient Assumptions for Non-interactive Zero-Knowledge Proofs of Knowledge for All NP Relations. Lecture Notes in Computer Science, 2000, , 451-462.	1.0	22
397	A New Anonymous Fingerprinting Scheme with High Enciphering Rate. Lecture Notes in Computer Science, 2001, , 30-39.	1.0	11
398	Perfectly Concealing Quantum Bit Commitment from any Quantum One-Way Permutation. Lecture Notes in Computer Science, 2000, , 300-315.	1.0	49
399	Oblivious Polynomial Evaluation and Oblivious Neural Learning. Lecture Notes in Computer Science, 2001, , 369-384.	1.0	42
400	The Representation Problem Based on Factoring. Lecture Notes in Computer Science, 2002, , 96-113.	1.0	18
401	Receipt-Free Sealed-Bid Auction. Lecture Notes in Computer Science, 2002, , 191-199.	1.0	31
402	Interactive Bi-Proof Systems and Undeniable Signature Schemes. , 1991, , 243-256.		20
403	Secure Computation. , 1991, , 392-404.		141
404	Cryptographically Strong Undeniable Signatures, Unconditionally Secure for the Signer. Lecture Notes in Computer Science, 1992, , 470-484.	1.0	104
405	All Languages in NP Have Divertible Zero-Knowledge Proofs and Arguments Under Cryptographic Assumptions. Lecture Notes in Computer Science, 1991, , 1-10.	1.0	10
406	Oblivious transfer protecting secrecy. Lecture Notes in Computer Science, 1991, , 31-45.	1.0	13
407	A General Zero-Knowledge Scheme. , 1989, , 122-133.		8
408	Sorting out zero-knowledge. , 1989, , 181-191.		10
409	Everything in NP can be argued in perfect zero-knowledge in a bounded number of rounds. , 1989, , 192-195.		13
410	Zero-Knowledge Proofs of Computational Power. , 1989, , 196-207.		9

#	Article	IF	Citations
411	More Efficient Match-Making and Satisfiability The Five Card Trick. Lecture Notes in Computer Science, 1990, , 208-217.	1.0	103
412	The Dining Cryptographers in the Disco: Unconditional Sender and Recipient Untraceability with Computationally Secure Serviceability. , 1989, , 690-690.		55
413	How to Break a â€œSecureâ€•Oblivious Transfer Protocol. , 1992, , 285-296.		15
414	Cryptographic Protocols Provably Secure Against Dynamic Adversaries. , 1992, , 307-323.		68
415	Perfect Zero-Knowledge Arguments for NP Can Be Based on General Complexity Assumptions. , 1992, , 196-214.		21
416	On the Discrepancy between Serial and Parallel of Zero-Knowledge Protocols. , 1992, , 246-259.		3
417	On Interactive Proofs with a Laconic Prover. Lecture Notes in Computer Science, 2001, , 334-345.	1.0	7
418	Interactive Hashing Simplifies Zero-Knowledge Protocol Design. , 1993, , 267-273.		11
420	Auditable, Anonymous Electronic Cash. Lecture Notes in Computer Science, 1999, , 555-572.	1.0	43
421	Language Dependent Secure Bit Commitment. , 1994, , 188-201.		5
422	Designated Confirmer Signatures and Public-Key Encryption are Equivalent. , 1994, , 61-74.		49
423	Coin-Based Anonymous Fingerprinting. Lecture Notes in Computer Science, 1999, , 150-164.	1.0	42
424	Proving in Zero-Knowledge that a Number is the Product of Two Safe Primes. Lecture Notes in Computer Science, 1999, , 107-122.	1.0	169
425	Adaptively Secure Oblivious Transfer. Lecture Notes in Computer Science, 1998, , 300-314.	1.0	9
426	Secure commitment against a powerful adversary. Lecture Notes in Computer Science, 1992, , 437-448.	1.0	7
427	Any language in IP has a divertible ZKIP. Lecture Notes in Computer Science, 1993, , 382-396.	1.0	7
428	Trials of traced traitors. Lecture Notes in Computer Science, 1996, , 49-64.	1.0	84
429	A progress report on subliminal-free channels. Lecture Notes in Computer Science, 1996, , 157-168.	1.0	17

#	Article	IF	Citations
430	Equivocable Oblivious Transfer. Lecture Notes in Computer Science, 1996, , 119-130.	1.0	7
431	Short Discreet Proofs. Lecture Notes in Computer Science, 1996, , 131-142.	1.0	11
432	Publicly Verifiable Secret Sharing. Lecture Notes in Computer Science, 1996, , 190-199.	1.0	294
433	Asymmetric Fingerprinting. Lecture Notes in Computer Science, 1996, , 84-95.	1.0	131
434	Round-Optimal Zero-Knowledge Arguments Based on Any One-Way Function. Lecture Notes in Computer Science, 1997, , 280-305.	1.0	37
435	Efficient Cryptographic Protocols Based on Noisy Channels. Lecture Notes in Computer Science, 1997, , 306-317.	1.0	92
436	Anonymous Fingerprinting. Lecture Notes in Computer Science, 1997, , 88-102.	1.0	100
438	A Taxonomy of Proof Systems. , 1997, , 109-134.		6
439	The Varieties of Secure Distributed Computation. , 1993, , 392-417.		13
440	Fair Games Against an All-Powerful Adversary. , 1993, , 418-429.		17
441	Secure Broadcast Communication. , 2003, , .		55
442	Non-Uniformly Sound Certificates with Applications to Concurrent Zero-Knowledge. Lecture Notes in Computer Science, 2019, , 98-127.	1.0	2
443	Lattice-Based Zero-Knowledge SNARGs for Arithmetic Circuits. Lecture Notes in Computer Science, 2019, , 217-236.	1.0	8
444	New Code-Based Privacy-Preserving Cryptographic Constructions. Lecture Notes in Computer Science, 2019, , 25-55.	1.0	13
445	Succinct Arguments in the Quantum Random Oracle Model. Lecture Notes in Computer Science, 2019, , 1-29.	1.0	29
446	SoK: Transparent Dishonesty: Front-Running Attacks on Blockchain. Lecture Notes in Computer Science, 2020, , 170-189.	1.0	66
447	Threshold Ring Signatures: New Definitions and Post-quantum Security. Lecture Notes in Computer Science, 2020, , 423-452.	1.0	6
448	Spartan: Efficient and General-Purpose zkSNARKs Without Trusted Setup. Lecture Notes in Computer Science, 2020, , 704-737.	1.0	76

#	Article	IF	Citations
449	Efficient Modular NIZK Arguments from Shift and Product. Lecture Notes in Computer Science, 2013, , 92-121.	1.0	10
450	Verifiable Computation with Reduced Informational Costs and Computational Costs. Lecture Notes in Computer Science, 2014, , 292-309.	1.0	4
451	Message Franking via Committing Authenticated Encryption. Lecture Notes in Computer Science, 2017, , 66-97.	1.0	37
452	Non-interactive Provably Secure Attestations for Arbitrary RSA Prime Generation Algorithms. Lecture Notes in Computer Science, 2017, , 206-223.	1.0	7
454	On the Security of Classic Protocols for Unique Witness Relations. Lecture Notes in Computer Science, 2018, , 589-615.	1.0	1
455	Collision Resistant Hashing for Paranoids: Dealing with Multiple Collisions. Lecture Notes in Computer Science, 2018, , 162-194.	1.0	25
457	On the Random-Oracle Methodology as Applied to Length-Restricted Signature Schemes. Lecture Notes in Computer Science, 2004, , 40-57.	1.0	40
458	On the Possibility of One-Message Weak Zero-Knowledge. Lecture Notes in Computer Science, 2004, , 121-132.	1.0	20
459	Zero-Knowledge Proofs and String Commitments Withstanding Quantum Attacks. Lecture Notes in Computer Science, 2004, , 254-272.	1.0	22
460	Efficient Unconditional Oblivious Transfer from Almost Any Noisy Channel. Lecture Notes in Computer Science, 2005, , 47-59.	1.0	59
461	Untraceable Fair Network Payment Protocols with Off-Line TTP. Lecture Notes in Computer Science, 2003, , 173-187.	1.0	9
462	Commitment Capacity of Discrete Memoryless Channels. Lecture Notes in Computer Science, 2003, , 35-51.	1.0	61
463	Succinct NP Proofs from an Extractability Assumption. Lecture Notes in Computer Science, 2008, , 175-185.	1.0	32
464	Perfect NIZK with Adaptive Soundness. , 2007, , 118-136.		53
465	Zero Knowledge and Soundness Are Symmetric. Lecture Notes in Computer Science, 2007, , 187-209.	1.0	11
466	Generic and Practical Resettable Zero-Knowledge in the Bare Public-Key Model. Lecture Notes in Computer Science, 2007, , 129-147.	1.0	21
467	Efficient Generic On-Line/Off-Line Signatures Without Key Exposure. Lecture Notes in Computer Science, 2007, , 18-30.	1.0	59
468	The Complexity of Zero Knowledge. Lecture Notes in Computer Science, 2007, , 52-70.	1.0	5

#	Article	IF	Citations
469	Off-Line/On-Line Signatures: Theoretical Aspects and Experimental Results. Lecture Notes in Computer Science, 2008, , 101-120.	1.0	26
470	An Equivalence Between Zero Knowledge and Commitments. , 2008, , 482-500.		25
471	Interactive and Noninteractive Zero Knowledge are Equivalent in the Help Model. , 2008, , 501-534.		15
472	On Constant-Round Concurrent Zero-Knowledge. , 2008, , 553-570.		18
473	Concurrent Non-malleable Commitments from Any One-Way Function. , 2008, , 571-588.		64
474	Which Languages Have 4-Round Zero-Knowledge Proofs?. , 2008, , 73-88.		18
475	Sub-linear Zero-Knowledge Argument for Correctness of a Shuffle. , 2008, , 379-396.		58
476	Quantum Cryptography. , 2012, , 1521-1543.		4
477	Classification Framework for Fair Content Tracing Protocols. Lecture Notes in Computer Science, 2009, , 252-267.	1.0	3
478	Chosen-Ciphertext Secure RSA-Type Cryptosystems. Lecture Notes in Computer Science, 2009, , 32-46.	1.0	6
479	An Efficient Parallel Repetition Theorem. Lecture Notes in Computer Science, 2010, , 1-18.	1.0	26
480	Concurrent Non-Malleable Zero Knowledge Proofs. Lecture Notes in Computer Science, 2010, , 429-446.	1.0	22
481	Improved Delegation of Computation Using Fully Homomorphic Encryption. Lecture Notes in Computer Science, 2010, , 483-501.	1.0	217
484	One-Time Signatures and Chameleon Hash Functions. Lecture Notes in Computer Science, 2011, , 302-319.	1.0	44
485	Fully Simulatable Quantum-Secure Coin-Flipping and Applications. Lecture Notes in Computer Science, 2011, , 21-40.	1.0	14
486	On the Efficiency of Bit Commitment Reductions. Lecture Notes in Computer Science, 2011, , 520-537.	1.0	9
487	A Note on (Im)Possibilities of Obfuscating Programs of Zero-Knowledge Proofs of Knowledge. Lecture Notes in Computer Science, 2011, , 292-311.	1.0	1
488	Point Obfuscation and 3-Round Zero-Knowledge. Lecture Notes in Computer Science, 2012, , 190-208.	1.0	32

#	Article	IF	Citations
489	Resettable Statistical Zero Knowledge. Lecture Notes in Computer Science, 2012, , 494-511.	1.0	13
490	Strictly-Black-Box Zero-Knowledge and Efficient Validation of Financial Transactions. Lecture Notes in Computer Science, 2012, , 738-749.	1.0	14
493	Domain-Specific Pseudonymous Signatures for the German Identity Card. Lecture Notes in Computer Science, 2012, , 104-119.	1.0	23
494	Allowing Non-identifying Information Disclosure in Citizen Opinion Evaluation. Lecture Notes in Computer Science, 2013, , 241-254.	1.0	6
495	Succinct Non-Interactive Zero Knowledge Arguments from Span Programs and Linear Error-Correcting Codes. Lecture Notes in Computer Science, 2013, , 41-60.	1.0	59
496	Secure Two-Party Computation with Reusable Bit-Commitments, via a Cut-and-Choose with Forge-and-Lose Technique. Lecture Notes in Computer Science, 2013, , 441-463.	1.0	23
497	Unconditionally Secure and Universally Composable Commitments from Physical Assumptions. Lecture Notes in Computer Science, 2013, , 100-119.	1.0	27
498	Computationally-Sound Proofs. Lecture Notes in Logic, 1998, , 214-268.	0.1	2
499	Tight Parallel Repetition Theorems for Public-Coin Arguments Using KL-Divergence. Lecture Notes in Computer Science, 2015, , 229-246.	1.0	7
500	Implicit Zero-Knowledge Arguments and Applications to the Malicious Setting. Lecture Notes in Computer Science, 2015, , 107-129.	1.0	15
501	Efficient Zero-Knowledge Arguments for Arithmetic Circuits in the Discrete Log Setting. Lecture Notes in Computer Science, 2016, , 327-357.	1.0	174
502	3-Message Zero Knowledge Against Human Ignorance. Lecture Notes in Computer Science, 2016, , 57-83.	1.0	11
503	On the (In)Security of SNARKs in the Presence of Oracles. Lecture Notes in Computer Science, 2016, , 108-138.	1.0	13
504	Interactive Oracle Proofs. Lecture Notes in Computer Science, 2016, , 31-60.	1.0	119
505	Chameleon-Hashes with Ephemeral Trapdoors. Lecture Notes in Computer Science, 2017, , 152-182.	1.0	68
506	The Hunting of the SNARK. Journal of Cryptology, 2017, 30, 989-1066.	2.1	51
507	Non-Interactive Zero-Knowledge for Blockchain: A Survey. IEEE Access, 2020, 8, 227945-227961.	2.6	37
508	How convincing is your protocol?. ACM SIGACT News, 1991, 22, 5-12.	0.1	6

#	Article	IF	Citations
509	A taxonomy of proof systems (part 1). ACM SIGACT News, 1993, 24, 2-13.	0.1	2
510	Asymmetric fingerprinting for larger collusions. , 1997, , .		65
511	Universally Composable Security. Journal of the ACM, 2020, 67, 1-94.	1.8	48
513	Classical zero-knowledge arguments for quantum computations. Quantum - the Open Journal for Quantum Science, 0, 4, 266.	0.0	8
514	Title is missing!. Theory of Computing, 2018, 14, 1-37.	0.3	29
515	Distributed Provers and Verifiable Secret Sharing Based on the Discrete Logarithm Problem. DAIMI Report Series, 1992, 21, .	0.1	18
516	Information-Theoretically Secure String Commitments Based on Packet Reordering Channels. IEEE Access, 2021, 9, 139928-139945.	2.6	0
517	DisCO: Peer-to-Peer Random Number Generator in Partial Synchronous Systems. , 2021, , .		0
518	Analysis and Design of E-voting Protocol. IFIP Advances in Information and Communication Technology, 2000, , 281-290.	0.5	0
519	How to Convert a Flavor of Quantum Bit Commitment. BRICS Report Series, 2000, 7, .	0.2	0
520	Equitability in Retroactive Data Confiscation versus Proactive Key Escrow. Lecture Notes in Computer Science, 2001, , 277-286.	1.0	1
521	Min-round Resettable Zero-Knowledge in the Public-Key Model. Lecture Notes in Computer Science, 2001, , 373-393.	1.0	15
522	A New Asymmetric Fingerprinting Framework Based on Secret Sharing. IFIP Advances in Information and Communication Technology, 2002, , 29-40.	0.5	0
523	Privacy for the Stock Market. Lecture Notes in Computer Science, 2002, , 269-288.	1.0	10
524	Probabilistically Checkable Proofs the Easy Way. , 2002, , 337-351.		2
525	The Dark Side of Threshold Cryptography. Lecture Notes in Computer Science, 2003, , 198-219.	1.0	3
526	On the Computational Collapse of Quantum Information. BRICS Report Series, 2003, 10, .	0.2	0
527	Proxy Confirmation Signatures. Informatica, 2004, 15, 425-437.	1.5	0

#	Article	IF	Citations
528	List-Decoding of Linear Functions and Analysis of a Two-Round Zero-Knowledge Argument. Lecture Notes in Computer Science, 2004, , 101-120.	1.0	1
530	Foundations of Modern Cryptography. , 2005, , 89-131.		2
531	You Can Prove So Many Things in Zero-Knowledge. Lecture Notes in Computer Science, 2005, , 10-27.	1.0	1
532	Chaumâ€™s Designated Confirmer Signature Revisited. Lecture Notes in Computer Science, 2005, , 164-178.	1.0	3
534	Non-interactive Designated Verifier Proofs and Undeniable Signatures. Lecture Notes in Computer Science, 2005, , 136-154.	1.0	8
535	Non-black-box Techniques in Cryptography. Lecture Notes in Computer Science, 2006, , 1-1.	1.0	7
536	Revisiting Colored Networks and Privacy Preserving Censorship. Lecture Notes in Computer Science, 2006, , 140-150.	1.0	2
537	ACM SIGACT news distributed computing column 24. ACM SIGACT News, 2006, 37, 58-84.	0.1	0
539	Reducing Complexity Assumptions for Statistically-Hiding Commitment*. SSRN Electronic Journal, 0, , .	0.4	0
540	Dissecting the Meaning of an Encrypted Message: An Approach to Discovering the Goals of an Adversary. Lecture Notes in Computer Science, 2008, , 61-72.	1.0	1
541	Efficient Concurrent n poly(logn)-Simulatable Argument of Knowledge. Lecture Notes in Computer Science, 2009, , 93-101.	1.0	0
542	Non-malleable Statistically Hiding Commitment from Any One-Way Function. Lecture Notes in Computer Science, 2009, , 303-318.	1.0	6
543	Efficient Deniable Authentication for Signatures. Lecture Notes in Computer Science, 2009, , 272-291.	1.0	7
544	Statistically-Hiding Quantum Bit Commitment from Approximable-Preimage-Size Quantum One-Way Function. Lecture Notes in Computer Science, 2009, , 33-46.	1.0	7
545	A Cryptographic Framework for the Controlled Release Of Certified Data. , 2010, , 33-56.		0
546	Key Generation for Fast Inversion of the Paillier Encryption Function. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2010, E93-A, 1111-1121.	0.2	0
547	Copyright Protection in the Distribution of Multimedia Digital Objects in Internet. Advances in Multimedia and Interactive Technologies Book Series, 2010, , 344-368.	0.1	0
549	Interactive Argument. , 2011, , 618-619.		0

#	Article	IF	Citations
550	A PUBLIC RANDOMNESS SERVICE. , 2011, , .		7
551	(Nearly) Round-Optimal Black-Box Constructions of Commitments Secure against Selective Opening Attacks. Lecture Notes in Computer Science, 2011, , 541-558.	1.0	8
552	A Secure and Practical Fingerprinting Protocol for Industry Design Map. Communications in Computer and Information Science, 2012, , 646-652.	0.4	0
553	Conoscenza nulla. Unitext, 2012, , 349-388.	0.0	0
554	Adaptive and Composable Non-interactive String-Commitment Protocols. Communications in Computer and Information Science, 2012, , 233-242.	0.4	0
555	Computazione a parti multiple. Unitext, 2012, , 389-422.	0.0	0
556	Round-Optimal Black-Box Statistically Binding Selective-Opening Secure Commitments. Lecture Notes in Computer Science, 2012, , 395-411.	1.0	2
557	Deniable RSA Signature. Lecture Notes in Computer Science, 2012, , 132-142.	1.0	0
558	A Cryptographic Moving-Knife Cake-Cutting Protocol. Electronic Proceedings in Theoretical Computer Science, EPTCS, 0, 78, 15-23.	0.8	2
559	From Selective-ID to Full-ID IBS without Random Oracles. Lecture Notes in Computer Science, 2013, , 172-190.	1.0	0
560	Why Philosophers Should Care about Computational Complexity. , 2013, , 261-328.		41
561	UC and EUC Weak Bit-Commitments Using Seal-Once Tamper-Evidence. Scientific Annals of Computer Science, 0, , 191-228.	0.4	0
563	An Efficient Elliptic Curve Discrete Logarithm based Trapdoor Hash Scheme without Key Exposure. Journal of Computers, 2013, 8, .	0.4	1
564	Obfuscation-Based Non-Black-Box Extraction and Constant-Round Zero-Knowledge Arguments of Knowledge. Lecture Notes in Computer Science, 2014, , 120-139.	1.0	2
565	Unbedingte Unbeobachtbarkeit mit kryptographischer Robustheit. Informatik-Fachberichte, 1987, , 302-320.	0.2	0
566	â€œPractical IPâ€•âŠ† MA. Lecture Notes in Computer Science, 1990, , 580-582.	1.0	0
567	Public-Randomness in Public-Key Cryptography. Lecture Notes in Computer Science, 1991, , 46-62.	1.0	10
568	On bit correlations among preimages of â€œMany to oneâ€•One-way functions. Lecture Notes in Computer Science, 1993, , 435-446.	1.0	0

#	Article	IF	Citations
569	An extension of zero-knowledge proofs and its applications. Lecture Notes in Computer Science, 1993, , 368-381.	1.0	1
570	A taxonomy of proof systems (part 2). ACM SIGACT News, 1994, 25, 22-30.	0.1	0
571	A Practical Conference Key Distribution System. IFIP Advances in Information and Communication Technology, 1995, , 167-175.	0.5	0
572	Kopierschutz durch asymmetrische SchlÃ¼sselkennzeichnung mit Signeten. , 1997, , 17-32.		1
573	A Relationship between One-Wayness and Correlation Intractability. Lecture Notes in Computer Science, 1999, , 82-96.	1.0	2
574	The Search for the Holy Grail in Quantum Cryptography. Lecture Notes in Computer Science, 1999, , 183-216.	1.0	1
575	On Zero-Knowledge with Strict Polynomial-Time Simulation and Extraction from Differing-Input Obfuscation for Circuits. Lecture Notes in Computer Science, 2015, , 51-68.	1.0	0
576	Three-Round Public-Coin Bounded-Auxiliary-Input Zero-Knowledge Arguments of Knowledge. Lecture Notes in Computer Science, 2015, , 130-149.	1.0	0
577	Efficient ID-based Non-Malleable Trapdoor Commitments Based on RSA and Factoring. Journal of Communications, 2015, , .	1.3	0
578	Efficient Zero-Knowledge Proofs of Knowledge of Double Discrete Logarithm. International Journal of Security and Its Applications, 2015, 9, 191-208.	0.5	1
579	On the Implausibility of Constant-Round Public-Coin Zero-Knowledge Proofs. Lecture Notes in Computer Science, 2016, , 237-253.	1.0	3
580	Efficient Generic Zero-Knowledge Proofs from Commitments (Extended Abstract). Lecture Notes in Computer Science, 2016, , 190-212.	1.0	1
581	Four-Round Zero-Knowledge Arguments of Knowledge with Strict Polynomial-Time Simulation from Differing-Input Obfuscation for Circuits. Lecture Notes in Computer Science, 2016, , 281-292.	1.0	0
582	Thrifty Zero-Knowledge. Lecture Notes in Computer Science, 2016, , 344-353.	1.0	0
583	Oblivious Transfer from Any Non-trivial Elastic Noisy Channel via Secret Key Agreement. Lecture Notes in Computer Science, 2016, , 204-234.	1.0	3
584	Generic Construction of Chameleon Hash to Group Elements. Journal of Communications, 2016, , .	1.3	0
585	Attacks on the Basic cMix Design: On the Necessity of Commitments and Randomized Partial Checking. Lecture Notes in Computer Science, 2017, , 463-473.	1.0	0
586	A Distributed Investment Encryption Scheme: Investcoin. Lecture Notes in Computer Science, 2017, , 136-154.	1.0	0

#	Article	IF	Citations
587	How to Challenge and Cast Your e-Vote. Lecture Notes in Computer Science, 2017, , 130-145.	1.0	7
589	On Round Optimal Statistical Zero Knowledge Arguments. Lecture Notes in Computer Science, 2019, , 128-156.	1.0	4
590	Unifying Computational Entropies via Kullbackâ€“Leibler Divergence. Lecture Notes in Computer Science, 2019, , 831-858.	1.0	4
591	On the Existence of Nash Equilibrium in Games with Resource-Bounded Players. Lecture Notes in Computer Science, 2019, , 139-152.	1.0	0
592	DELEGATING COMPUTATION VIA NO-SIGNALING STRATEGIES. , 2019, , .		0
593	On Succinct Arguments and Witness Encryption from Groups. Lecture Notes in Computer Science, 2020, , 776-806.	1.0	8
594	A review on smart metering infrastructure. International Journal of Energy Technology and Policy, 2020, 16, 277.	0.1	0
596	Post-quantum Resettably-Sound Zero Knowledge. Lecture Notes in Computer Science, 2021, , 62-89.	1.0	1
597	Generic Construction of Anonymous Deniable Predicate Authentication Scheme with Revocability. Lecture Notes in Computer Science, 2020, , 142-155.	1.0	0
598	Unprovability of Leakage-Resilient Cryptography Beyond the Information-Theoretic Limit. Lecture Notes in Computer Science, 2020, , 621-642.	1.0	0
599	Fully Collision-Resistant Chameleon-Hashes from Simpler and Post-quantum Assumptions. Lecture Notes in Computer Science, 2020, , 427-447.	1.0	2
600	On Statistical Security in Two-Party Computation. Lecture Notes in Computer Science, 2020, , 532-561.	1.0	5
601	Individual Simulations. Lecture Notes in Computer Science, 2020, , 805-836.	1.0	3
602	Bringing Order to Chaos: The Case of Collision-Resistant Chameleon-Hashes. Lecture Notes in Computer Science, 2020, , 462-492.	1.0	9
603	Redactable Transactions in Consortium Blockchain: Controlled by Multi-authority CP-ABE. Lecture Notes in Computer Science, 2021, , 408-429.	1.0	9
604	Black-Box Impossibilities of Obtaining 2-Round Weak ZK and Strong WI from Polynomial Hardness. Lecture Notes in Computer Science, 2021, , 369-400.	1.0	1
605	ROSEN. , 2021, , .		2
606	Tandem: Securing Keys by Using a Central Server While Preserving Privacy. Proceedings on Privacy Enhancing Technologies, 2020, 2020, 327-355.	2.3	0

#	Article	IF	Citations
607	Concurrent Statistical Zero-Knowledge Arguments for NP from One Way Functions. , 2007, , 444-459.		5
608	Review of Techniques for Privacy-Preserving Blockchain Systems. , 2020, , .		10
610	Finding Collisions in Interactive Protocols - A Tight Lower Bound on the Round Complexity of Statistically-Hiding Commitments. , 2007, , .		2
611	Argus: A Fully Transparent Incentive System for Anti-Piracy Campaigns. , 2021, , .		0
612	SoK. , 2021, , .		13
613	On the Commitment Capacity of Reverse Elastic Channels. , 2021, , .		4
614	Limbo: Efficient Zero-knowledge MPCitH-based Arguments. , 2021, , .		6
616	Is it Easier to Prove Theorems that are Guaranteed to be True?. , 2020, , .		4
617	On Commitment over General Compound Channels. , 2022, , .		2
618	SNARGs for $mathcal{P}$ from LWE. , 2022, , .		9
619	Irrationality, Extortion, or Trusted Third-parties: Why it is Impossible to Buy and Sell Physical Goods Securely on the Blockchain. , 2021, , .		7
620	Updatable Linear Map Commitments and Their Applications in Elementary Databases. , 2021, , .		0
621	ProvNet: Networked bi-directional blockchain for data sharing with verifiable provenance. Journal of Parallel and Distributed Computing, 2022, 166, 32-44.	2.7	8
624	Constant-Round Leakage-Resilient Zero-Knowledge from Collision Resistance. Journal of Cryptology, 2022, 35, 1.	2.1	0
625	Succinct Non-Interactive Arguments via Linear Interactive Proofs. Journal of Cryptology, 2022, 35, 1.	2.1	6
626	Zero-Knowledge IOPs withÂLinear-Time Prover andÂPolylogarithmic-Time Verifier. Lecture Notes in Computer Science, 2022, , 275-304.	1.0	10
627	Online-Extractability inÂtheÂQuantum Random-Oracle Model. Lecture Notes in Computer Science, 2022, , 677-706.	1.0	17
628	Multi-Server Verifiable Computation of Low-Degree Polynomials. , 2022, , .		8

#	Article	IF	Citations
629	A Gift that Keeps on Giving: The Impact of Public-Key Cryptography on Theoretical Computer Science. , 2022, , 157-184.		0
630	Characterizing sustainability materiality: ESG materiality determination in technology venturing. , 2022, 1, 100024.		4
631	What Makes Fiatâ€"Shamir zkSNARKs (Updatable SRS) Simulation Extractable?. Lecture Notes in Computer Science, 2022, , 735-760.	1.0	8
632	Forward-Secure Revocable Secret Handshakes fromÂLattices. Lecture Notes in Computer Science, 2022, , 453-479.	1.0	3
633	Verifiable Relation Sharing andÂMulti-verifier Zero-Knowledge inÂTwo Rounds: Trading NIZKs withÂHonest Majority. Lecture Notes in Computer Science, 2022, , 33-56.	1.0	6
634	Secret handshakes: Full dynamicity, deniability and lattice-based design. Theoretical Computer Science, 2023, 940, 14-35.	0.5	2
635	Privacy-Preserving and Publicly Verifiable Matrix Multiplication. IEEE Transactions on Services Computing, 2022, , 1-13.	3.2	2
636	Round-Optimal Honest-Majority MPC in Minicrypt andÂwith Everlasting Security. Lecture Notes in Computer Science, 2022, , 103-120.	1.0	2
637	Relationship of Socioeconomic Status with Special Reference to Leucorrhoea. , 0, , 203-208.		0
638	FairBlock: Preventing Blockchain Front-Running withÂMinimal Overheads. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2023, , 250-271.	0.2	1
639	Concurrently Composable Non-interactive Secure Computation. Lecture Notes in Computer Science, 2022, , 526-555.	1.0	0
640	Comparison of current blockchain privacy protection technologies and prospects for future trends. , 2023, , .		0
641	On-Line/Off-Line DCR-Based Homomorphic Encryption andÂApplications. Lecture Notes in Computer Science, 2023, , 115-131.	1.0	0
642	When Arthur Has Neither Random Coins Nor Time to Spare: Superfast Derandomization of Proof Systems. , 2023, , .		1
643	Constant-Round Arguments from One-Way Functions. , 2023, , .		0
644	Retractable Commitment over Noisy Channels. , 2023, , .		0
645	Impossibilities inÂSuccinct Arguments: Black-Box Extraction andÂMore. Lecture Notes in Computer Science, 2023, , 465-489.	1.0	1
646	Non-interactive Zero-Knowledge fromÂNon-interactive Batch Arguments. Lecture Notes in Computer Science, 2023, , 38-71.	1.0	0

#	Article	IF	Citations
647	Individual Cryptography. Lecture Notes in Computer Science, 2023, , 547-579.	1.0	0
649	Fides: A System forÂVerifiable Computation Using Smart Contracts. Lecture Notes in Computer Science, 2023, , 448-480.	1.0	0
651	Cost-Efficient Anonymous Authentication Scheme Based on Set-Membership Zero-Knowledge Proof. , 2023, , .		0
652	Zero-Knowledge Systems fromÂMPC-in-the-Head andÂOblivious Transfer. Lecture Notes in Computer Science, 2024, , 120-136.	1.0	0
653	Secure and Decentralized Generation of Secret Random Numbers on the Blockchain. , 2023, , .		1
654	Commitments withÂEfficient Zero-Knowledge Arguments fromÂSubset Sum Problems. Lecture Notes in Computer Science, 2024, , 189-208.	1.0	0
655	zkFDL: An efficient and privacy-preserving decentralized federated learning with zero knowledge proof. , 2024, , .		0
656	Cryptographic Primitives. Advances in Information Security, 2024, , 25-72.	0.9	0
657	Interactive Argument. , 2024, , 1-1.		0